

strongSwan IPsec VPN Client for Android 4.0

User Manual

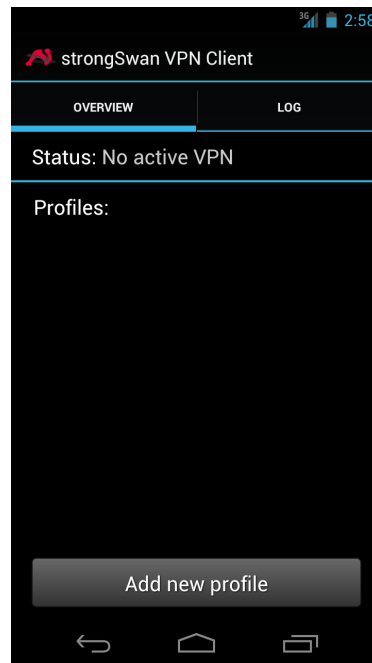
June 15, 2012



Contents

1 Introduction	2
2 Creating a VPN Profile	3
3 Starting a VPN Connection	6
4 Editing or Deleting a Profile	10
5 Reading the Logs	11
6 Installing your own CA Certificates	12

1 Introduction

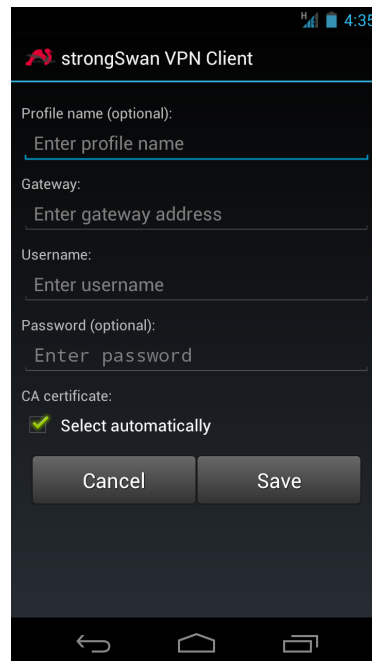


When the strongSwan VPN client is started on the device, the first thing you will see is the overview screen. It is divided into three sections: the navigation bar at the top, the status section right below and the list of profiles, which is initially empty, at the bottom.

The navigation bar lets you switch between the overview and the log view. The status section indicates whether or not a VPN is currently established. Read the next section to learn how to create a new VPN profile.

2 Creating a VPN Profile

You can add a new profile by pressing the *Add new profile* button at the bottom of the screen. A new view will pop up where you can enter the settings for the new profile:

A screenshot of the 'strongSwan VPN Client' application interface. The screen is dark-themed and displays several input fields for creating a new profile. At the top, the title 'strongSwan VPN Client' is visible. Below it, the fields are: 'Profile name (optional):' with a placeholder 'Enter profile name'; 'Gateway:' with a placeholder 'Enter gateway address'; 'Username:' with a placeholder 'Enter username'; 'Password (optional):' with a placeholder 'Enter password'; and 'CA certificate:' with a checked checkbox and the text 'Select automatically'. At the bottom of the form are two buttons: 'Cancel' and 'Save'. The Android navigation bar is visible at the very bottom.

Profile name

This is the profile name which will be shown on the overview. It is only used locally and can be chosen freely. If you leave this field blank, the Gateway address is used as name for the profile.

Gateway

This is the address (hostname or IP address) of the gateway you wish to connect to.

Username

Your username (EAP)

Password

Your password for the EAP-MD5 or EAP-MSCHAPv2 authentication. You can choose not to enter the password. In that case, you will be asked to enter your password on each attempt to start the VPN connection.

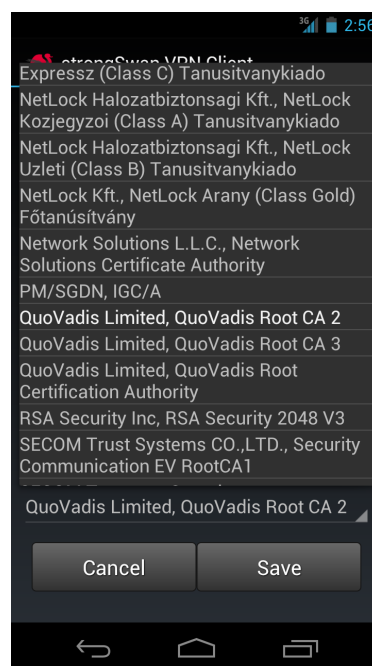
CA Certificate

The CA certificate which is used for the gateway authentication.

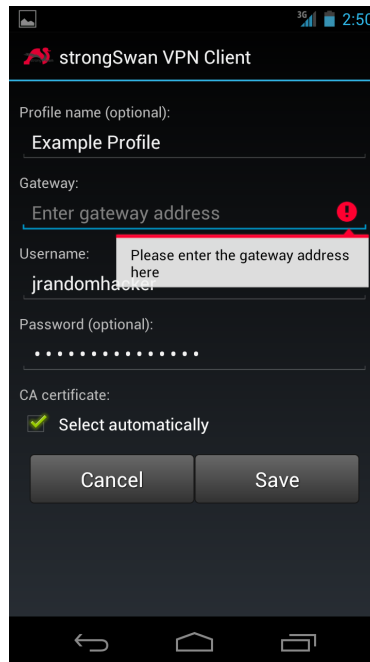
You can either let strongSwan automatically pick the CA certificate that is needed to authenticate the gateway or you can manually select the one to be used.

Note that in case you choose *Select automatically*, strongSwan sends a certificate request for every CA certificate installed on the device to the gateway, which may be slow or cause problems with packet fragmentation.

If you choose to select the CA certificate manually, you can select it from the drop-down menu that will show up. Note that per default, only certificates that were manually installed by the user are shown. If you want to see the pre-installed CA certificates as well, select *Show all certificates*. See [section 6](#) on how to install your own certificate on the device.

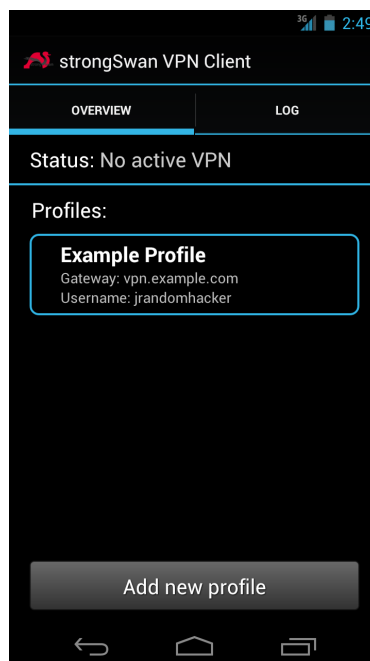


When you have filled in all the necessary fields, you can save the profile by pressing the *Save* button. Otherwise, you will be prompted to enter the missing information (as shown below)



You can then adjust the missing parameter and press the *Save* button again.

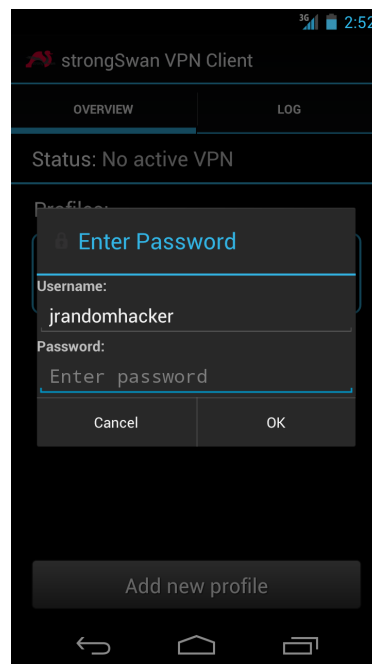
After you have successfully created a new VPN profile, it will show up in the list of profiles:



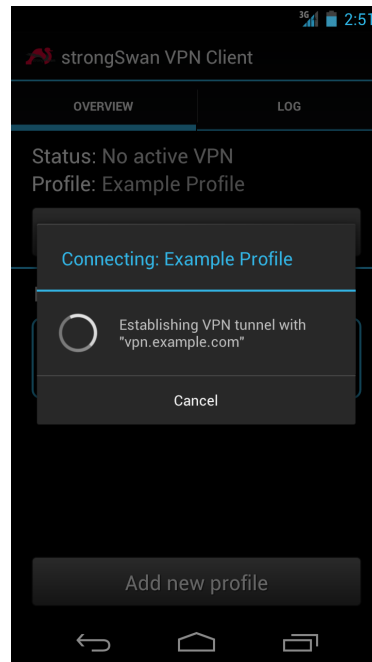
3 Starting a VPN Connection

After you created a profile, you can activate the profile simply by tapping it.

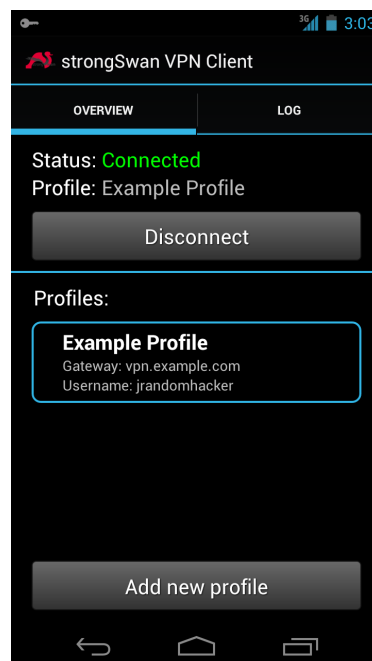
If you did not enter your password when you created the profile, you will be asked to enter it now:



Then, a dialog will pop up while strongSwan tries to establish the connection to the VPN gateway:

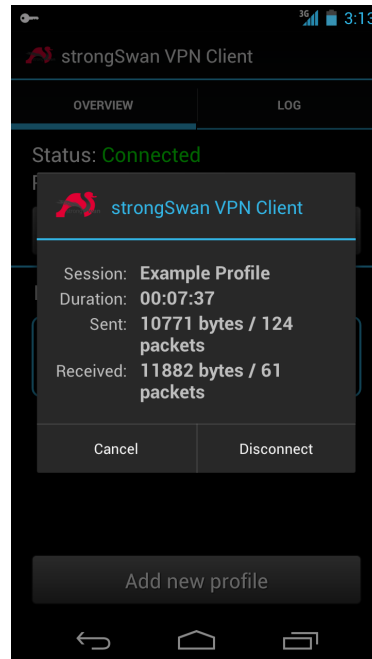


You can press *Cancel* to abort the connection attempt. After the VPN Tunnel is established, a bell sound is played and the status will be changed to *Connected*:

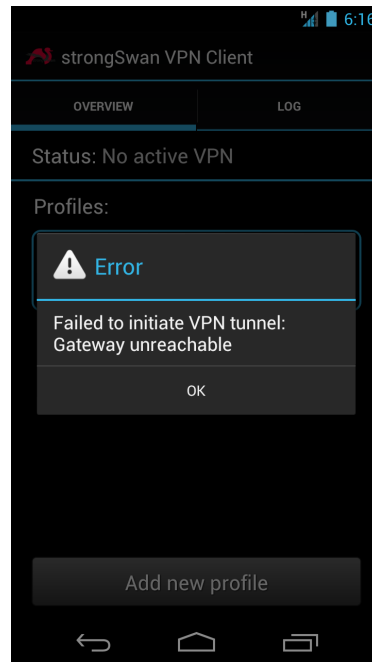


If you wish to terminate the VPN at any time, press the *Disconnect* button.

A small key icon in the notification area at the top of the screen indicates that a VPN connection is active even if the strongSwan app is not visible. If you open the notification, you can see more details about the currently active connection:



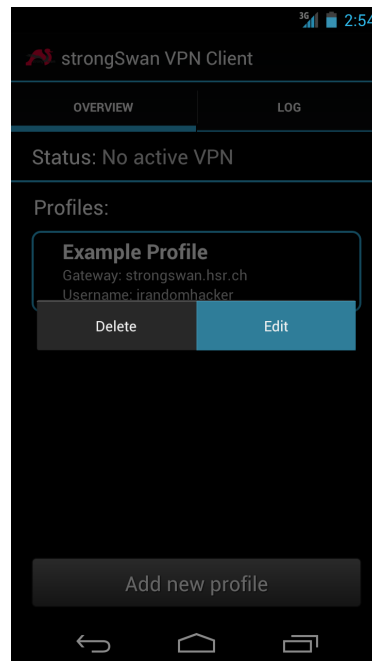
If an error occurred and the VPN could not be established, a message will pop up describing the error, e.g.:



If you are looking for more detailed information about an error, you can also take a look at the log messages generated by strongSwan (see [section 5](#)).

4 Editing or Deleting a Profile

In order to edit an existing VPN profile, press on the profile you wish to edit and hold until your device vibrates. A small dialog will pop up:

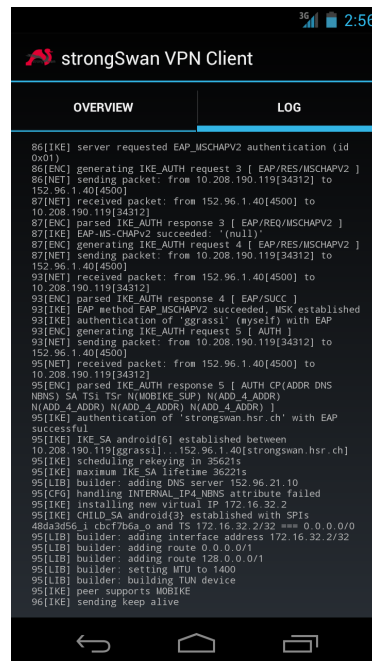


You can choose to either delete or edit the profile. If you press *Edit*, the profile detail view will show up. There, you can edit all the parameters of the profile. See also [section 2](#).

After you finished editing the profile, press the *Save* button to adapt your changes, or press *Cancel* if you want to discard the changes.

5 Reading the Logs

If you are an expert and want to read the logs generated by strongSwan, select the *Log* tab or swipe horizontally over the screen of your device.



The log view automatically scrolls to the latest log message. You can use the log for example to diagnose problems or to look at the traffic selectors in order to see what traffic is sent over the tunnel.

To return to the *Overview* you can use the tabs or swipe the screen again in the opposite direction.

6 Installing your own CA Certificates

If you have your own CA certificate that you want to use with the strongSwan VPN client, you have to install it as a trusted certificate on the device.

In order to do that, you need to copy the DER-encoded certificate onto your SD card. Note that the file name of the certificate needs a `.cer` ending, otherwise it will not be recognized by Android. After you have inserted the SD card, go to *Settings*→*Security*→*Credential Storage*→*Install from SD card*. If you do not yet have a pin or screen lock pattern set for your device, you will be prompted to configure one now. Afterwards the certificate will be installed on the device. You will then be able to see the certificate when editing a VPN profile.